



**The right item, right place,
right time.**

Privacy Act 101 Privacy Awareness Training

**AUDIENCE: DLA Workforce Annually
(Civilian employees, Military members, and DLA Contractors)**



Topics to be Addressed

- What is the Privacy Act?
- Rights Granted Individuals
- DLA's Responsibilities
- Individuals Covered
- Records Subject to the Act
- System of Record Notice
- Privacy Act Statement
- **PENALTIES**
- Accessing Your Records
- Privacy Act Exemptions
- What Else Should You Know?
- "Rules of Conduct"
- "Code of Fair Information Principles"
- Summary & Questions
- Available Privacy Training
- For More Info, Contact . . .
- Certificate



What is the Privacy Act?

The Privacy Act (5 U.S.C. 552a), passed by Congress in 1974, establishes certain controls over what personal information is collected and maintained by the Executive Branch of the federal government, and how the information is used. The Act grants certain rights to an individual on whom records are maintained, and assigns responsibilities to an agency which maintains the information.



Who is Subject to the Privacy Act provisions?

The entire DLA Workforce (civilian employees, military members, and DLA contractors) is subject to the Privacy Act and must comply with all of its provisions.

Non-compliance with the Privacy Act carries **criminal** and **civil** penalties.



What Rights Are Granted Individuals Under the Privacy Act?

Under the Act, individuals are granted the right to:

- Determine what records about them are being collected, maintained, used, or disseminated by DLA;
- Prevent records pertaining to them from being used or made available for another purpose without their consent;
- Gain access to records about oneself, subject to Privacy Act exemptions;
- Amend a record if it is inaccurate, irrelevant, untimely, or incomplete; and
- Sue the government for violations of the statute, such as permitting unauthorized individuals access to your records.



What Are DLA's Responsibilities under the Privacy Act?

DLA's responsibilities include:

- Maintaining only such information that is both relevant and necessary to accomplish a purpose of the agency required to be accomplished by Federal statute or by Executive Order;
- Collecting information to the greatest extent practicable directly from the subject individual;
- Informing each individual whom it asks to supply information with a Privacy Act Statement;
- Publishing the existence of a system of records (and subsequent changes thereto), i.e., system of records notice;
- Maintaining all records used by the agency about an individual with such accuracy, relevance, timeliness, and completeness to assure fairness to the individual;



What Are DLA's Responsibilities Under the Privacy Act? (cont'd)

DLA's responsibilities include:

- Maintaining no record describing how any individual exercises their First Amendment rights, unless authorized by law.
- Establishing “rules of conduct” for persons involved in the design, development, operation, or maintenance of any system of records; and the consequences of non-compliance. *DLA's Privacy “rules of conduct” are provided later in this module.*
- Establishing appropriate physical, technical, and administrative safeguards for the security and accuracy of records to prevent substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. *Safeguarding Privacy Act Data is further addressed in Privacy Act 103 training module.*



What Individuals are Covered by the Privacy Act?

The Privacy Act applies only to records collected and maintained on **living** individuals* who are:

- U.S. citizens or
- lawfully admitted aliens

whose records are filed in a “system of records” where those records are retrieved by a personal identifier.

** Corporations, partnerships, sole proprietorships, professional groups, businesses, whether incorporated or unincorporated, and other commercial entities **are not** “individuals.”*



What Records are Subject to the Privacy Act?

Records subject to the Privacy Act are those about an individual collected and maintained in a “system of records.” A system of records is a group of records that:

- Contains a personal identifier (such as a name, date of birth, Social Security Number, Employee Number, fingerprint, etc.);
- Contains at least one other item of personal data (such as home address, performance rating, blood type, etc.); and
- The data about the subject individual **IS** retrieved by their personal identifier(s).

The Privacy Act **DOES NOT** apply to information about individuals in records that are filed under other subjects, such as organizations or events, unless the agency also indexes and retrieves the information by an individual’s name or other personal identifier.



What is a Privacy Act “System of Records Notice”

DLA is required by the Privacy Act to publish the existence of a system of records in the *Federal Register*; this is called a “system of records notice” also known as SORN. The notice:

- Informs the general public what data is being collected, the purpose of the collection, and the authority for doing so; and
- Sets the rules that DLA will follow in collecting and maintaining the personal data.

DLA has published approximately 80 Privacy Act systems of records notices which are available at <http://www.dod.mil/privacy/notices/dla>.

DOD, as a whole, has published approximately 1200 systems of records notices which are available at <http://www.dod.mil/privacy/notices>.



Additional Systems of Records Notices

DLA also maintains records on individuals under government-wide systems of records notices. As the name indicates, these are systems of records notices published by other federal agencies which have responsibility for records which are applicable government-wide. These systems of records notices are available at <http://www.dod.mil/privacy/govwide>. Federal agencies which have published these types of systems of records notices include:

- Office of Personnel Management
- Equal Employment Opportunity Commission
- General Services Administration
- Merit Systems Protection Board
- Department of Labor
- Federal Emergency Management Agency
- Office of Government Ethics

All Federal agency Privacy Act systems of records notices can be found at <http://www.gpoaccess.gov/privacyact/index.html>



System of Records Notice (SORN) Elements

Elements of a Privacy Act system of records notice:

- System identifier:
- System name:
- System location:
- Categories of individuals covered by the system:
- Categories of records in the system:
- Authority for maintenance of the system:
- Purpose(s):
- Routine uses of records maintained in the system, including categories of users and the purposes of such uses:
- Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:
- Storage:
- Retrievability:
- Safeguards:
- Retention and disposal:
- System manager(s) and address:
- Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:
- Storage:
- Retrievability:
- Safeguards:
- Retention and disposal:
- System manager(s) and address:
- Notification procedure:
- Record access procedures:
- Contesting record procedures:
- Record source categories:
- Exemptions claimed for the system:

Contact your local **Privacy Act Officer** for assistance in drafting your SORN.



What is a Privacy Act Statement?

When an individual is requested to furnish personal information about themselves for inclusion in a Privacy Act system of records, the individual must be provided a Privacy Act Statement (PAS). The PAS enables the individual to make an informed decision whether to provide the requested information, and the consequences if they choose not to provide the information. The elements of a PAS are:

Privacy Act Statement

Authority: Identifies the specific Federal statute or Executive Order that authorizes the collection of information;

Purpose(s): Identifies the internal DLA / DOD uses made of the information;

Routine Uses: Identifies the entities outside DLA / DOD who will have access to the data, and the uses made of the information;

Disclosure: Is the information provided voluntary or mandatory, and the effects on the individual if they choose not to provide the requested information;

Rules of Use: DLA added this element to its PAS to identify for the individual the applicable Privacy Act system of records notice.



Are there Penalties for Violating the Privacy Act?

Criminal and civil penalties are addressed in the Privacy Act for non-compliance. You personally may be liable if you knowingly and willfully:

- Obtaining or requesting records under false pretenses.
- Disclosing privacy data to any person not entitled to access.
- Maintaining a system of records without meeting public notice requirements.



PENALTY:

Misdemeanor criminal charge and a fine of up to **\$5000** (for each offense) and/or administrative sanctions.



Penalties (cont'd)

Courts may also award civil penalties against DLA for:

- Improperly / unlawfully refusing to amend a record.
- Improperly / unlawfully refusing to grant access to a record.
- Failure to maintain accurate, relevant, timely, and complete information.
- Failure to comply with any Privacy Act provision or agency rule that results in an adverse effect on the subject of the record.

Penalties for these violations include:

- Actual damages
- Payment of reasonable attorney's fees
- Removal from employment





How Do I Access My Records Contained in a System of Records?

Requests for information about you contained in a DLA Privacy Act system of records must:

- Be in writing and signed.
- Be addressed to the appropriate DLA activity you believe is maintaining the information about you.
- Identify the applicable DLA Privacy Act system of records notice that might contain the information you are seeking, and your relationship with DLA and the time period of that relationship. DLA Privacy Act systems of records notices are found at <http://www.dod.mil/privacy/notices/dla>.
- Provide any other documentation as listed under the Notification or Access elements within the Privacy Act system of records notice.
- When in doubt, contact your local Privacy Act Officer.



Privacy Act Exemptions

Under the Privacy Act, there are 10 exemptions under which DLA can withhold certain kinds of information from you. Examples of exempt records are those containing classified information on national security and those concerning criminal investigations. The 10 exemptions DLA may claim are provided below.

- 5 U.S.C. 552a(c)(3) - covers release to the record subject of certain accountings of disclosure. This exemption is a self-executing.
- 5 U.S.C. 552a(d)(5) - information compiled in reasonable anticipation of a civil action or proceeding. This exemption is self-executing.



Privacy Act Exemptions (cont'd)

- 5 U.S.C. 552a(j)(2) - selected records maintained by an agency or component whose principal function is any activity pertaining to the criminal law enforcement. *DLA may not claim this exemption.*
- 5 U.S.C. 552a(k)(1) - records systems containing information properly classified in the interest of national defense or foreign policy.
- 5 U.S.C. 552a(k)(2) - investigatory material compiled for law enforcement purposes *other than* material covered by 5 U.S.C. 552a(j)(2).
- 5 U.S.C. 552a(k)(3) - records systems maintained in connection with providing protective services to the President of the United States or other individuals who received protection from the Secret Service.



Privacy Act Exemptions (cont'd)

- 5 U.S.C. 552a(k)(4) - records systems required by statute to be maintained and used *solely* as statistical records.
- 5 U.S.C. 552a(k)(5) - investigatory material compiled *solely* to determine suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information.
- 5 U.S.C. 552a(k)(6) - records systems that contain testing or examination material used *solely* to determine individual qualifications for appointment or promotion in the Federal, but only when disclosure would compromise the objectivity or fairness of the testing or examination process.
- 5 U.S.C. 552a(k)(7) - evaluation material used to determine potential for promotion in the armed services.



Is This All I Need to Know About the Privacy Act?

That depends on what your job entails. Privacy Officers, Web/Database Developers, IT System Managers, Privacy Act system managers, as well as those individuals who work with Privacy Act data should seek additional training. Contact your local Privacy Act Officer and/or access additional training modules on the [DLA eFOIA webpage](#).

As a member of the DLA workforce, you should also be familiar with:

- The DLA Privacy “Rules of Conduct”
- The DLA “Code of Fair Information Principles”



What are the DLA Privacy “Rules of Conduct?”

The Privacy Act requires each agency to establish “rules of conduct” for all persons involved in the design, development, operation, and maintenance of a Privacy Act system of records, and the **penalties** for non-compliance.

As a member of the DLA Workforce, **YOU** play an important role in assuring that DLA complies with the provisions of the Privacy Act.



DLA Privacy Rules of Conduct (cont'd)

The DLA Workforce shall:

- Ensure that personal information contained in a system of records, to which they have access to or are using incident to the conduct of official business, shall be protected so that the security and confidentiality of the information shall be preserved.
- Not disclose any personal information contained in any system of records except as authorized. Personnel willfully making such a disclosure when knowing that disclosure is prohibited are subject to possible criminal penalties and/or administrative sanctions.
- Report any unauthorized disclosures of personal information from a system of records or the maintenance of any system of records that are not authorized to your local Privacy Act Officer or to your supervisor.



DLA Privacy Rules of Conduct (cont'd)

DLA Privacy Act System Managers shall:

- Ensure that all personnel who either shall have access to the system of records or who shall develop or supervise procedures for handling records in the system of records shall be aware of their responsibilities for protecting personal information being collected and maintained under the DLA Privacy Program.
- Prepare promptly any required new, amended, or altered systems notices for the system of records and submit them through the DLA HQ Privacy Officer for publication in the *Federal Register*.
- Not maintain any official files on individuals that are retrieved by name or other personal identifier without first ensuring that a Privacy Act system of records notice has been published in the *Federal Register*. Any official who willfully maintains a system of records without meeting the publication requirements of the Privacy Act is subject to possible criminal penalties and/or administrative sanctions.



Rules of Conduct Helpful Hints

Helpful Hints:



Mark Privacy Act protected records appropriately.

“For Official Use Only - Privacy Act Data”



Report any unauthorized disclosures of personal information from a system of records to your Privacy Act Officer.



Collect the minimum amount of personally identifiable information necessary for the proper performance of a documented agency function.

REMINDER:

Privacy Act non-compliance carries penalties.





Rules of Conduct

Helpful Hints (cont'd)

Helpful Hints:

- ❌ Do not collect personal information without proper authorization.
- ❌ Do not place Privacy Act protected information on shared drives, multi-access calendars, the Intranet (eWorkplace), or the Internet.
- ❌ Challenge ANYONE who asks to see Privacy Act information for which you are responsible.
- ❌ Do not commingle / mix information about different individuals in the same file within a system of records.
- ❌ Do not maintain records longer than permitted **OR** destroy records before disposal requirements are met.



Rules of Conduct Helpful Hints (cont'd)

Helpful Hints:

- ❌ Do not use interoffice or translucent envelopes to mail Privacy Act protected data. Instead, use sealable opaque solid white or Kraft envelopes. Be sure to mark the envelope to the person's attention.
- ❌ Do not distribute or release personal information to other employees unless you are convinced that the release is authorized / proper.
- ❌ Do not create a "system of records" on your computer, or in your files without first contacting your local Privacy Act Officer.
- ❌ Do not place unauthorized documents in systems of records.



“Code of Fair Information Principles”

In order to assure that any personal information submitted to DLA is properly protected, DLA has devised a list of principles to be applied when handling personal information. This is referred to as the “**Code of Fair Information Principles.**”

The **Code** is set forth in a list of 10 policies that the DLA Workforce will follow when handling personal information. Any member of the DLA Workforce who handles the personal information of others must abide by the principles set forth by the **Code.**



“Code of Fair Information Principles” (cont’d)

- 1. The Principle of Openness:** When we collect personal data from you, we will inform you of the intended uses of the data, the disclosures that will be made, the authorities for the collection, and whether the collection is mandatory or voluntary. We will collect no data subject to the Privacy Act unless a Privacy Act system of records notice has been published in the *Federal Register*.
- 2. The Principle of Individual Participation:** Unless an exemption has been claimed from the Privacy Act, we will, upon request, grant you access to your records; provide you a list of disclosures made outside the DOD; and make corrections to your file, once shown to be in error.
- 3. The Principle of Limited Collection:** DLA will collect only those personal data elements required to fulfill an official function or mission grounded in law. Those collections are conducted by lawful and fair means.



“Code of Fair Information Principles” (cont’d)

- 4. The Principle of Limited Retention:** DLA will retain your personal information only as long as necessary to fulfill the purposes for which it is collected, and then destroy it.
- 5. The Principle of Data Quality:** DLA strives to maintain only accurate, relevant, timely, and complete data about you.
- 6. The Principle of Limited Internal Use:** DLA will use your personal data only for lawful purposes, and limit access to those individuals with an official need for access.
- 7. The Principle of Disclosure:** The DLA Workforce will zealously guard your personal data to ensure that all disclosures are made with your written permission or are made in strict accordance with the Privacy Act.



“Code of Fair Information Principles” (cont’d)

8. The Principle of Security: Your personal data is protected by appropriate physical, administrative, and technical safeguards to ensure security and confidentiality.

9. The Principle of Accountability: DLA and the DLA Workforce are subject to civil and criminal penalties for certain breaches of Privacy. DLA is diligent in sanctioning individuals who violate the Privacy Act.

10. The Principle of Challenging Compliance: You may challenge DLA if you believe that DLA has failed to comply with these principles, the Privacy Act, or the system of records notice.



Summary

Each and every member of the DLA Workforce needs to be aware of their responsibilities under the Privacy Act to protect the security of personal information; ensure its accuracy, relevance, timeliness, and completeness; avoid unauthorized disclosures either orally or in writing; and ensure that no system of records retrieved by personal identifier is maintained without prior public notice in the *Federal Register*.

Through increased awareness DLA can effectively balance openness with protection of individual privacy and remain responsive to the public's interest in Government.



QUESTION

The Privacy Act applies to all personal data collected and maintained by the Federal Government.

TRUE

FALSE



ANSWER

FALSE. The Privacy Act applies only to personal data collected and maintained by the Executive branch of the Federal Government, about U.S. citizens and lawfully admitted aliens, and only if the records are maintained in a “system of records.”



QUESTION

Penalties associated with violating the Privacy Act can only be imposed against the agency; nothing will happen to me personally.

TRUE

FALSE



ANSWER

FALSE. The Privacy Act carries penalties that can be levied against **YOU**, i.e., a misdemeanor criminal charge and a fine of up to **\$5000** (for each offense), and/or removal from employment.



QUESTION

Safeguarding Privacy Act data is the job of each and every member of the DLA Workforce.

TRUE

FALSE



ANSWER

TRUE. The DLA Workforce are stewards of information. We have an affirmative responsibility to ensure that Privacy Act information is collected, maintained, used, and disseminated only as authorized by law and regulation and that the information is continually safeguarded.



Available Privacy Training

Additional information about the Privacy Act can be obtained by visiting the DLA eFOIA/Privacy Act Office webpage at

http://www.dla.mil/public_info/efoia/Training.html.



For More Information, Contact

DLA Headquarters Privacy Act Officer

Ms. Jody Sinkler

Headquarters, Defense Logistics Agency, ATTN: DP
8725 John J. Kingman Road, Stop 2533
Fort Belvoir, VA 22060-6221

COM 703 767-5045

DSN 427-5045

FAX 703 767-5283



Certificate of Completion

Congratulation on the completion of

Privacy Act 101

Privacy Awareness Training

Mandatory Annual training for the DLA Workforce

(Civilian employees, Military members, and DLA Contractors)